National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

NARA Bulletin 2007-02 **April 30, 2007**

TO: Heads of Federal agencies

SUBJECT: Guidance concerning the use of Enterprise Rights Management (ERM) and other encryption-related software on Federal records

EXPIRATION DATE: April 30, 2010

1. What is the purpose of this bulletin? This bulletin provides guidance to Federal agencies on records management implications of their use of enterprise rights management (ERM) and other software employing encryption technologies. It advises agencies that:

- Use of ERM and other encryption-related software on permanent records is prohibited at time of transfer of legal custody to NARA; and

- Use of these technologies on temporary records can impede and in some cases abrogate traditional records management controls.

2. What is enterprise rights management? Enterprise rights management (ERM) software manages and enforces information access policies and use rights of electronic documents within an enterprise; its development has been predicated on digital rights management (DRM) technology. Digital rights management (DRM) was developed to provide a systematic approach to copyright protection for digital content, generally by means of a suite of software employing the following technologies: identity/role management, privilege management, tamper-detection, and cryptography. Using ERM, creators of digital content may assign rights to future users to take subsequent actions on that ERM-protected content (e.g., opening, printing, editing, copying, or forwarding the content).

3. How does ERM work? ERM is established on an organization's policy server as a set of "rules" that are applied to content created in that environment. Rules specify the rights of individual users to take actions on particular digital content. When users operating in such an environment create content requiring ERM, they apply rules from the policy server (e.g., "Allow this memo to be edited by members of my workgroup during the next 3 days, but do not allow the memo to be shared outside of this group. At the end of 3 days, automatically dispose of all copies.") The selected rules applied to a piece of digital content are then unalterably bound to that content. When other individuals attempt to access that content, the client software contacts the policy server to verify those individuals' access rights. ERM-protected content can easily be identified by information in the file header.

4. How does encryption work? Encryption is a technology that may be deployed independent of ERM. It is the conversion of data into a form, called ciphertext that cannot be easily understood by unauthorized people. This reversible conversion process, which is basically a mathematical transformation of the underlying bitstream, is accomplished by use of a "key." Keys are long prime numbers that are input into the encryption algorithm to either encode or decode the data. Encrypted records are easily recognized in their ciphertext state as they are unintelligible.

5. Why is NARA concerned about the use of these technologies? Application of ERM or encryption technologies to digital Federal records could impair the ability of agencies to fulfill records management responsibilities under 36 CFR 1228.10.

6. How do ERM and encryption technologies impact agencies' records management obligations? A variety of records management concerns are evoked by the use of ERM technology to digital Federal record content. These include:

- "Expirations" of documents set by individual creators might be in conflict with authorized retention periods;
- Without appropriate policies in place, an agency might receive ERM-protected materials generated outside of the government (e.g., contractors, business, the Public) which do not afford sufficient rights to the Government to conduct its business using that material (e.g., FDA drug applications);
- Application of inappropriate or outdated rules to ERM-protected content may result in the records being inaccessible when needed for agency business;
- The hardware/software-dependence of ERM protected materials may make it difficult to ensure access to long-term records to which this technology is applied; or
- Keys belonging to individuals encrypting files may be lost (e.g., through negligence or employee turnover), thereby resulting in the potential loss of access to Government record information.

7. If my agency deploys ERM or encryption technologies, what advice does NARA have? NARA suggests agencies choosing to deploy ERM or encryption technologies take steps to evaluate the effect that this will have on records management practices and consider instituting policies and procedures that will minimize adverse consequences. These could include:

- Not applying ERM protections to permanent Federal records.
- Establishing ERM screening mechanisms for received content originating outside the agency.
- Providing training to content creators so that rights and conditions assigned to content are in agreement with agency records schedules.

- Where possible, establishing default rights and conditions at the ERM server which are in agreement with disposition authorities and preventing these from being overridden at the content creator's desktop.

- Developing business cases for deployment of ERM technology that adequately fund maintenance of long-term, ERM-protected materials.

- Establishing key recovery/escrow mechanisms and procedures that will ensure access to encryption keys applied to agency records during the entirety of their active lifespan.

8. Will NARA accept permanent records with attached ERM policies? No. As part of the accessioning process, NARA will routinely scan electronic records during accessioning for ERM protection. If such content is encountered, the records will be rejected and returned to the originating agency for removal of the ERM protection.

9. Why is NARA prohibiting the use of ERM and encryption technologies to permanent records it legally accessions? NARA's holdings need to be preserved and made accessible, in perpetuity, to a variety of users. Use of these technologies on permanent materials is antagonistic to that mission: escrow and recovery of keys used to encrypt records would also substantially complicate access. Furthermore, in-house maintenance of ERM platforms is not only prohibitively expensive, but also contrary to software/hardware independence objectives of the Electronic Records Archives program.

10. What actions must agencies take prior to transfer of permanent records to which ERM or encryption technologies has been applied? If agencies have either encrypted or applied ERM controls to permanent Federal records, it is their responsibility to remove such controls on the record copies before they are transferred to NARA. If this capability is not inherent to the ERM or encryption environment, automated processes will have to be developed to remove ERM protections from bodies of records prior to transfer to NARA. Records that have been encrypted may only be transferred in an unencrypted state.

11. Is assistance available from NARA?

a. NARA's Life Cycle Management Division provides assistance and advice to agency records officers in the Washington, DC, area. Your agency's records officer may contact the NARA appraiser or records analyst with whom your agency normally works. A list of the appraisal and scheduling work groups is posted on the NARA web site at http://www.archives.gov/records_management/policy_and_guidance/appraisal_and_scheduling.html.

b. The Records Management staff in NARA's regional offices provides assistance to records officers across the country. A complete list of NARA regional facilities may be found at http://www.archives.gov/facilities/index.html.

c. If you need more general information about the contents of this bulletin, please contact Mark Giguere, Lead IT (Policy & Planning) for Modern Records Programs at mark.giguere@nara.gov or on 301-837-1744.

ALLEN WEINSTEIN
Archivist of the United States